DATA BREACHES ARE INEVITABLE — OR ARE THEY?

The average total cost of a typical data breach in the U.S.:

$5.4 MILLION

SOME COST MUCH MORE.

A data breach can take a toll on a company of any size. Here's a look at some significant data breaches, tips to protect your business, and what to do in the event of a data breach.

SOME FAMOUS HACKING CASES

2007
At least **46 million** TJ Maxx Companies customers were affected by a breach.

2008
Info from **130 million** credit and debit card customers was stolen from Heartland Payment Systems, whose customer included 7-Eleven.

2011
Sony said that sensitive information for **77 million** people was placed at risk.

2012
Adobe Systems said personal data for nearly **38 million** customers was hacked.

2013
40 million credit card numbers were stolen from Target Corp.

2013
1 million credit card accounts at Neiman Marcus were hacked.

2014
56 million credit card numbers at Home Depot were hacked.

2015
The Trump Hotel Collection, Hilton Worldwide, and Starwood hotels all said data had been compromised for periods beginning in **2014 and stretching into 2015.**

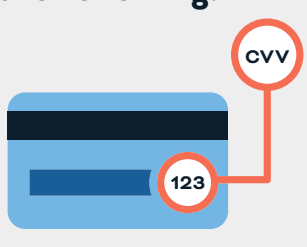
2016
The personal information for **one billion** Yahoo! accounts was hacked, making it the most expansive databreach thus far.

Small and midsized business are not immune. Cybercriminals steal an estimated $1 billion annually from these businesses in the U.S. and Europe, and 72% of those that suffer major data loss shut down within 24 months.

WHAT YOU CAN DO

Preventative tools can help you avoid being a victim. Ensure your payment processor has the following:

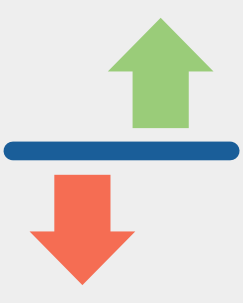
ON-HOLD FUNCTIONALITY
Transactions exceeding set parameters do not get processed until they are reviewed and approved.



CVV FILTER
Three- or four-digit code on card must be accurately entered during transaction.

VELOCITY FILTER
Transactions exceeding a specific quantity threshold are declined.

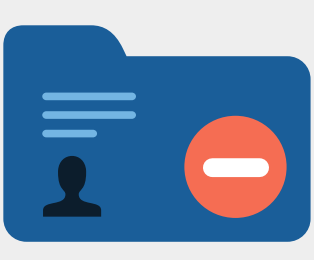
CARD ISSUING COUNTRY
Transactions from countries deemed untrustworthy can be blocked.



THRESHOLD
Transaction amounts over or under set amounts are declined.

GEO IP TRACKING
Transactions from specific IP addresses can be blocked.

ADDRESS VERIFICATION (AVS) FILTER
Address info provided during sale must match what bank has on file.



NEGATIVE DATABASE
Keep or subscribe to a database of identified fraudsters.

HOW YOUR BUSINESS SHOULD RESPOND TO A BREACH

Contact your attorney for guidance, and your merchant account provider.

Record date and time of breach discovery, and when response efforts begin.

Alert and activate response team.

Secure the area where the breach occurred to help preserve evidence.

Stop additional data loss, taking affected computers offline. Let the forensic team investigate and decide whether to shut them off.

Document all information known about the breach: Times; type of breach; what data was stolen; names of those who discovered breach, those alerted, and those debriefed, etc.

Review protocols about disseminating information about the breach.

Assess priorities and risks.

Have your forensics firm begin its investigation.

Notify law enforcement, if needed, after consulting with legal counsel and upper management.

Every business, no matter what the size, needs to partner with a credit card processor who has the tools and expertise to help them become PCI compliant and certified to protect their business. In today's ever-evolving credit card world, no business should be storing any sensitive payment data in its system.